CLAIMS

1- Method to secure the execution of a program in an electronic assembly comprising information processing means and information storage means, characterised in that it consists in checking the execution time of at least one sequence of said program with respect to the normal predetermined execution time of said sequence.

2- Method according to claim 1, characterised in that it consists in checking during the execution of at least one sequence of said program that the execution time of said sequence corresponds to the normal predetermined execution time of said sequence.

3- Method according to claim 1 or 2, characterised in that it consists in checking the point of arrival of said sequence on expiry of the normal predetermined execution time of said sequence.

4- Method according to one of claims 1 to 3, characterised in that it consists in checking that the execution of said sequence is at the planned point of arrival on expiry of the normal predetermined execution time of said sequence.

5- Method according to one of claims 1 to 4, characterised in that it consists in checking the execution time of at least one sequence of said program with respect to the normal predetermined execution time of said sequence so as to protect against attacks disturbing the execution of said program.

6- Method according to one of claims 1 to 5, characterised in that it consists in triggering at the start of said sequence an interrupt counter initialised to the value of the normal predetermined execution time of said sequence, in triggering an interrupt in the program execution on expiry of the

counter and in diverting execution of said program to an interrupt management routine in order to check the point of arrival of said sequence.

7- Method according to one of the previous claims, characterised in that if the execution time of said sequence is not normal, the interrupt management routine is immediately followed by a sequence to set a fraud indicator in memory or by an interruption of the current execution by another means.

8- Method according to one of the previous claims, characterised in that it consists in adding to said sequence instructions or loops or equivalent so as to equalise the execution time of the sequence in all its branches or so that the execution time of said sequence is modified if there is an attack.

9- Method according to claim 6, characterised in that the interrupt management routine is placed at the last location of the program memory or just before a shared domain boundary so as to leave the permitted program memory area if an attack prevents execution of the interrupt return.

10- Electronic module comprising information processing means and information storage means containing a program to be executed, characterised in that it comprises means to check the execution time of at least one sequence of said program with respect to the normal predetermined execution time of said sequence.

11 – Module according to claim 10, characterised in that the means comprise a counter with triggering of an interrupt on expiry.

12- Card characterised in that it comprises the electronic module according to claim 10 or 11.

13 - Computer program including program code instructions to execute steps of the method according to one of claims 1 to 9 when said program is run in a computer system.